EXHIBIT B

No.

IN THE
Supreme Court of the United States

FACEBOOK, INC., AND TWITTER, INC.,

Petitioners,

v.

SUPERIOR COURT OF SAN FRANCISCO COUNTY, DERRICK D. HUNTER, AND LEE SULLIVAN,

Respondents.

On Petition for a Writ of Certiorari to the California Court of Appeal

PETITION FOR A WRIT OF CERTIORARI

MICHAEL J. HOLECEK
THOMAS F. COCHRANE
GIBSON, DUNN & CRUTCHER LLP
333 South Grand Avenue
Los Angeles, CA 90071
(213) 229-7000

JOSHUA S. LIPSHUTZ
Counsel of Record
NAIMA L. FARRELL
AARON SMITH
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Avenue, N.W.
Washington, D.C. 20036
(202) 955-8500
jlipshutz@gibsondunn.com

Counsel for Petitioners
[Additional counsel listed on signature page]

QUESTION PRESENTED

Under the Stored Communications Act ("SCA"), covered service providers "shall not knowingly divulge to any person or entity the contents" of their account holders' communications, absent an applicable exception. 18 U.S.C. § 2702(a). The question presented is:

Whether a criminal defendant has a constitutional right to subpoena service providers and force them to turn over the contents of their account holders' communications, notwithstanding the SCA's express prohibition on such disclosures; and whether a service provider can be held in contempt for refusing to violate the SCA in response to such a subpoena.

PARTIES TO THE PROCEEDING AND RULE 29.6 STATEMENT

The parties named in the caption were parties to the proceeding below. Instagram, LLC was also a party to the proceedings below, but has since become a wholly-owned subsidiary of Facebook, Inc.

Pursuant to this Court's Rule 29.6, undersigned counsel state that Petitioner Facebook, Inc. is a publicly traded corporation. Facebook has no parent company. No publicly held company owns 10% or more of Facebook's stock. Undersigned counsel further state that Petitioner Twitter, Inc. is a publicly traded corporation. Twitter has no parent company. No publicly held company owns 10% or more of Twitter's stock.

RULE 14.1(b)(iii) STATEMENT

- *Facebook, Inc. et al. v. Superior Court of San Francisco County; Derrick D. Hunter et al.*, No. S257384 (Cal.) (judgment and order entered Sept. 11, 2019).
- *Facebook, Inc. et al. v. Superior Court for the City and County of San Francisco; Derrick D. Hunter et al.*, No. A157902 (Cal. Ct. App.) (judgment and order entered July 30, 2019).
- *People of the State of California v. Lee Sullivan & Derrick Hunter*, Nos. 13035657 & 13035658 (Cal. Superior Ct.) (judgment and order of contempt entered July 26, 2019).
- *Facebook, Inc. et al. v. Superior Court of San Francisco County; Derrick D. Hunter et al.*, No. S256686 (Cal.) (judgment and order dissolving stay entered July 17, 2019).
- *Facebook, Inc. et al. v. Superior Court for the City and County of San Francisco; Derrick D. Hunter et al.*, No. A157143 (Cal. Ct. App.) (judgment and order dissolving stay and order to show cause entered July 1, 2019).
- *Facebook, Inc. et al. v. Superior Court of the City and County of San Francisco; Derrick D. Hunter et al.*, No. S230051 (Cal.) (judgment and opinion issued May 24, 2018).
- *Facebook, Inc. et al. v. Superior Court of the City and County of San Francisco; Derrick D. Hunter et al.*, No. A144315 (Cal. Ct. App.) (judgment and opinion issued Sept. 8, 2015).

There are no additional proceedings in any court that are directly related to this case.

TABLE OF CONTENTS

Page

QUESTION PRESENTED....i
PARTIES TO THE PROCEEDING AND RULE 29.6 STATEMENT ii
RULE 14.1(b)(iii) STATEMENT.... iii
TABLE OF CONTENTS iv
TABLE OF APPENDICES v
TABLE OF AUTHORITIES....vi
PETITION FOR A WRIT OF CERTIORARI 1
OPINIONS BELOW....1
JURISDICTION 1
STATUTORY PROVISIONS INVOLVED 1
STATEMENT 1
REASONS FOR GRANTING THE PETITION 9
I. THE LOWER COURTS ARE DIVIDED ON THE PRIVACY PROTECTIONS AFFORDED BY THE STORED COMMUNICATIONS ACT....11
II. THIS CASE THREATENS THE PRIVACY INTERESTS OF MILLIONS OF AMERICANS. 15
CONCLUSION 22

TABLE OF APPENDICES

Page

APPENDIX A: Order of the California Supreme Court (Sept. 11, 2019).....1a

APPENDIX B: Order of the California Court of Appeals (July 30, 2019) 2a

APPENDIX C: Order and Judgment of Contempt of the Superior Court of California (July 26, 2019).....3a

APPENDIX D: Opinion of the California Supreme Court (May 24, 2018) 85a

APPENDIX E: Constitutional and Statutory Provisions Involved.....164a

U.S. Const. amend. V.....164a

U.S. Const. amend. VI 164a

18 U.S.C. § 2702.....165a

18 U.S.C. § 2703.....169a

18 U.S.C. § 2707.....179a

APPENDIX F: Examples of cases in which criminal defense subpoenas were issued to Facebook or Instagram since 2017 .....182a

TABLE OF AUTHORITIES

Page(s)

Cases

Abrams v. Johnson,
521 U.S. 74 (1997) 19

California v. Harris,
No. 19012702 (S.F. Super. Ct. Nov. 1, 2019) 14

California v. Rocha,
No. 180118907 (S.F. Super. Ct. Aug. 27, 2019) 14

Carpenter v. United States,
138 S. Ct. 2206 (2018) 16

Delaware v. Fensterer,
474 U.S. 15 (1985) 12

Eldred v. Ashcroft,
537 U.S. 186 (2003) 19

Facebook, Inc. v. Wint,
199 A.3d 625 (D.C. 2019) 10, 11, 12

Gun Owners' Action League, Inc. v. Swift,
284 F.3d 198 (1st Cir. 2002) 19

Hately v. Watts,
917 F.3d 770 (4th Cir. 2019) 4

Katz v. Liberty Power Corp.,
No. 18-cv-10506, 2019 WL 957129
(D. Mass. Feb. 27, 2019) 20

Mafille v. Kaiser-Francis Oil Co.,
No. 18-cv-586, 2019 WL 1933747
(N.D. Okla. May 1, 2019).....20

Michigan v. Bay Mills Indian Cmty.,
572 U.S. 782 (2014).....20

Montana v. Egelhoff,
518 U.S. 37 (1996).....12

Packingham v. North Carolina,
137 S. Ct. 1730 (2017).....16

Pennsylvania v. Ritchie,
480 U.S. 39 (1987).....12

PPG Indus., Inc. v. Jiangsu Tie Mao Glass Co.,
273 F. Supp. 3d 558 (W.D. Pa. 2017) 20

Riley v. California,
573 U.S. 373 (2014).....16

Salazar v. Buono,
559 U.S. 700 (2010).....19

Sines v. Kessler,
No. 18-mc-80080, 2018 WL 3730434
(N.D. Cal. Aug. 6, 2018).....20

State v. Bray,
422 P.3d 250 (Or. 2018) 10, 12, 13

State v. Johnson,
538 S.W.3d 32 (Tenn. Crim. App. 2017) 17

United States v. Freeze,
784 F. App'x 203 (5th Cir. 2019) 16

United States v. LaCoste,
821 F.3d 1187 (9th Cir. 2016) 16

United States v. Microsoft Corp.,
138 S. Ct. 1186 (2018) 15

United States v. Nix,
251 F. Supp. 3d 555 (W.D.N.Y. 2017) 17

United States v. Pierce,
785 F.3d 832 (2d Cir. 2015) 10, 13, 14

United States v. Scheffer,
523 U.S. 303 (1998) 12

United States v. Wenk,
319 F. Supp. 3d 828 (E.D. Va. 2017) 17

Statutes

18 U.S.C. § 2516 21

18 U.S.C. § 2702(a) 2, 5, 11

18 U.S.C. § 2702(b) 5, 7, 11

18 U.S.C. § 2703 ..... 5, 11

18 U.S.C. § 2707 ..... 5, 20

Rules

Cal. Rules of Court, Rule 8.532(b)(2)(A) 1

Other Authorities

Albert Gidari, *The Mandatory Emergency Disclosure Sinkhole Exception to the Email Privacy Act*, Ctr. for Internet & Society (May 24, 2016) 18

Allen D. Hankins, *Compelling Disclosure of Facebook Content Under the Stored Communications Act*, 17 Suffolk J. Trial & App. Advoc. 295 (2012) 6

Colin Fieman & Alan Zarky, *When Acquittal Is Just a Tweet Away: Obtaining Historical Social Media Evidence from Service Providers that Use the SCA as a Shield*, Champion 26 (Nov. 2015) 21

Facebook, *Government Requests for User Data* (2018), https://transparency.facebook.com/government-data-requests 6

Facebook, *Messenger*, https://www.messenger.com/ 16

H.R. Rep. No. 99-647 (1986) 4, 5, 18

Joshua A.T. Fairfield & Erik Luna, *Digital Innocence*, 99 Cornell L. Rev. 981 (2014) 20

Marc J. Zwillinger & Christian S. Genetski, *Criminal Discovery of Internet Communications Under the Stored Communications Act: It's Not a Level Playing Field*, 97 J. Crim. L. & Criminology 569 (2007) 21

Maura Dolan, *After that $5-Billion Fine, Facebook Gets Dinged Again*, L.A. Times (July 26, 2019) 14

Maura Dolan, *California Supreme Court Says Social Media Firms Must Turn Over Some User Communications to Criminal Defendants*, L.A. Times (May 24, 2018) 17

Maura Dolan, *In Unprecedented Move, Facebook, Instagram, Twitter Ordered to Provide Private Posts in Gang Trial*, L.A. Times (July 18, 2019) 14

Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208 (2004) 3, 5

Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 Colum. L. Rev. 279, 293 (2005) 17

Pew Research Ctr., *Internet/Broadband Fact Sheet* (June 12, 2019), https://tinyurl.com/wy3bh5h.....16

Press Release, *Facebook Reports Fourth Quarter and Full Year 2019 Results* (Jan. 29, 2020), https://tinyurl.com/topb9ok 6

Rebecca Wexler, *Evidence in the Age of Privacy: Access to Data in the Criminal Justice System*, 67 UCLA L. Rev. (forthcoming 2020) 21

Ryan A. Ward, *Discovering Facebook: Social Network Subpoenas and the Stored Communications Act*, 24 Harv. J.L. & Tech. 563 (2011) 6, 17

S. Rep. No. 99-541 (1986).....4, 5, 17, 18, 19

Stephanie Lacambra, *A Constitutional Conundrum That's Not Going Away—Unequal Access to Social Media Posts*, Electronic Frontier Foundation (May 31, 2018).....21

Twitter, *About Direct Messages*, https://help.twitter.com/en/using-twitter/direct-messages 16

Twitter, *Information Requests* (2018), https://transparency.twitter.com/en/information-requests.html.....6

Twitter, *Q4 2019 Letter to Shareholders* (Feb. 6, 2020), https://tinyurl.com/s63hklf 6

PETITION FOR A WRIT OF CERTIORARI

Petitioners Facebook, Inc. and Twitter, Inc. respectfully petition for a writ of certiorari to review the judgment of the California Court of Appeal.

OPINIONS BELOW

The disposition of the California Supreme Court (Pet. App. 1a) is unreported. The order of the California Court of Appeal (Pet. App. 2a) is unreported. The California Superior Court's order and judgment of contempt (Pet. App. 3a–84a) is unreported.

JURISDICTION

The California Court of Appeal entered its judgment on July 30, 2019. Pet. App. 2a. The California Supreme Court denied a petition for review on September 11, 2019. Pet. App. 1a; Cal. Rules of Court, Rule 8.532(b)(2)(A). On December 2, 2019, this Court extended the time for Petitioners to file their petition for a writ of certiorari until February 8, 2020. *See* No. 19A609. The jurisdiction of this Court is invoked under 28 U.S.C. § 1257.

STATUTORY PROVISIONS INVOLVED

Relevant provisions of the Constitution and the Stored Communications Act are reproduced in the Appendix. Pet. App. 164a–81a.

STATEMENT

The Stored Communications Act ("SCA") protects the privacy of millions of Americans. The statute commands that service providers like Facebook and Twitter who route and store electronic communications—including, for example, emails, Facebook posts, messages on Twitter, and Instagram communications—"shall not" divulge to third parties the contents of

their users' communications, except in limited circumstances prescribed by the SCA. 18 U.S.C. § 2702(a). This provision is intended to ensure that the content of communications remains protected from disclosure, thereby encouraging people to connect and share with each other and incentivizing technology companies to develop innovative ways for people to communicate.

Congress enacted the SCA in 1986, before the advent of social media, but the importance of the statute's protections has only increased since then, as electronic communications have become common occurrences in our everyday lives. These federal statutory protections, in turn, have spawned ever-increasing litigation over the ability of criminal defendants armed with a subpoena to access other people's communications—typically those of the crime victim and government witnesses—in search of potentially exculpatory evidence.

The lower courts are divided on the answer. The Second Circuit, the District of Columbia Court of Appeals, and the Oregon Supreme Court have each recognized the SCA's unambiguous command that service providers like Petitioners are prohibited from divulging communications absent a statutory exception, and have rejected criminal defendants' attempts to access other people's communications with a subpoena. As those courts have recognized, the SCA's prohibition on disclosure makes no exception for criminal defendants and does not pose any threat to criminal defendants' constitutional rights, in part because there are other means of obtaining the same communications—for example, directly from the participants to the communications at issue.

In the decisions below, however, the California courts upheld a contempt order against Facebook and

Twitter based on their refusal to violate the SCA and turn over their users' communications in response to criminal defendants' subpoenas. In holding Petitioners in contempt of court and fining Petitioners $1,000 apiece, the Superior Court found that the criminal defendants' Confrontation Clause and Due Process rights outweighed Congress's command.

That decision has sweeping implications. It undermines the SCA by eroding users' trust that their communications will be disclosed only in prescribed circumstances. It arms criminal defendants with the right to access the private messages of crime victims and witnesses through a subpoena to service providers—behind the backs of the people whose communications are at issue, and often with no opportunity for them to object to the violation of their privacy. It puts service providers in an impossible position, forcing them to choose between violating federal law or facing contempt for protecting users' communications as Congress instructed. And it places courts in charge of balancing the alleged interests of criminal defendants against competing privacy interests and burdens on service providers and the people who use their services—a balance that Congress already struck through its unambiguous SCA prohibition.

This Court should grant certiorari to resolve the split among lower courts and bring clarity to this important issue affecting the privacy interests of millions of Americans.

1. The Stored Communications Act filled a "gap" in Fourth Amendment doctrine that left electronic communications potentially unprotected from third-party access. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1210

(2004). Although the content of mailed letters and telephone calls received strong Fourth Amendment protections, electronic communications arguably did not. Congress recognized this problem in 1986, when many "American citizens and American businesses" had begun using computers to communicate "in lieu of, or side-by-side with," traditional methods of communication. S. Rep. No. 99-541, at 5 (1986). "With the advent of computerized recordkeeping systems, Americans ha[d] lost the ability to lock away a great deal of personal and business information." *Id.* at 3. Individuals' electronic communications were "open to possible wrongful use and public disclosure by law enforcement authorities as well as unauthorized private parties," and the providers of electronic services could "do little ... to resist." *Id*.

The legal uncertainty regarding the security of electronic communications posed several concerns. Because "potential customers have less protection when they use an electronic medium than with paper, there may be a disincentive to use an electronic service." H.R. Rep. No. 99-647, at 26 (1986). The uncertainty affected commercial interests, too, by "discourag[ing] American businesses from developing new innovative forms of telecommunications and computer technology." S. Rep. No. 99-541, at 5. And the legal gap "probably encourages unauthorized users to obtain access to communications to which they are not a party." *Id.*; *see also Hately v. Watts*, 917 F.3d 770, 783 (4th Cir. 2019) (examining the statutory background).

For these reasons, Congress enacted the SCA "to protect privacy interests in personal and proprietary information." S. Rep. No. 99-541, at 3. The "heart of the SCA" is the protections contained in 18 U.S.C.

§§ 2702 and 2703. Kerr, *A User's Guide to the SCA*, 72 Geo. Wash. L. Rev. at 1218.

Under the SCA, covered service providers "shall not knowingly divulge to any person or entity the contents" of electronic communications. 18 U.S.C. § 2702(a). The SCA enumerates certain "[e]xceptions" under which providers "may divulge" the contents of a communication, *id.* § 2702(b)—for example, if the sender or recipient of the communication consents to disclosure, *id.* § 2702(b)(3). The SCA also provides procedures by which the government can "require the disclosure" of the contents of a communication. *Id.* § 2703. This three-part scheme—prohibited disclosures, permitted disclosures, and mandatory disclosures—"represent[ed] a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement." S. Rep. No. 99-541, at 5.

The flat prohibition on disclosure included in Section 2702(a) was crucial to the SCA. "This provision reflects the rapidly growing importance of information storage and processing to the Nation's commerce." H.R. Rep. No. 99-647, at 65–66. "The secure storage of electronic information has thus become as important to the commercial system as the protection of paper records." *Id.* at 66. Congress accordingly gave the SCA teeth, codifying it in the federal criminal code and imposing significant liability on providers who knowingly violate the law. Any "person aggrieved by any violation" of the SCA can seek statutory damages, punitive damages, equitable relief, and attorneys' fees. 18 U.S.C. § 2707(a)–(c).

2. Facebook and Twitter are electronic communication service providers and/or remote computing service providers subject to the Stored Communications

Act. Facebook has 2.5 billion monthly active users. Press Release, *Facebook Reports Fourth Quarter and Full Year 2019 Results* (Jan. 29, 2020), https://tinyurl.com/topb9ok. Twitter has 152 million daily active users. Twitter, *Q4 2019 Letter to Shareholders* (Feb. 6, 2020), https://tinyurl.com/s63hklf. "The explosive growth of these sites has resulted in users creating an immense amount of online communications between one another on an ongoing basis." Allen D. Hankins, *Compelling Disclosure of Facebook Content Under the Stored Communications Act*, 17 Suffolk J. Trial & App. Advoc. 295, 295 (2012).

Communications on Facebook and Twitter sometimes contain information potentially relevant to law enforcement needs. Facebook and Twitter received a combined 97,610 requests for user account information from government entities in 2018. Facebook, *Government Requests for User Data* (2018), transparency.facebook.com/government-data-requests; Twitter, *Information Requests* (2018), transparency.twitter.com/en/information-requests.html. But private parties also seek user communications and records for litigation purposes. In 2018 alone, Twitter received 405 requests from private litigants, including criminal defendants, seeking the communications of 1,733 different user accounts. Twitter, *Information Requests*, *supra*; *see also* Pet. App. 182a–85a (collecting cases in which Facebook or Instagram received a criminal defense subpoena). Both Facebook and Twitter, like other electronic service providers, rely on the SCA to protect their users' communications. "Without the SCA, ... there is little to protect users from aggressive litigants ... who wish to access their social network information." Ryan A. Ward, *Discovering Facebook: Social Network Subpoenas and the Stored Communications Act*, 24 Harv. J.L. & Tech. 563, 565 (2011).

3. In 2014, Defendants Derrick Hunter and Lee Sullivan were awaiting trial for murder and other crimes stemming from an alleged drive-by shooting. They subpoenaed Petitioners for all content from Facebook, Instagram, and Twitter accounts belonging to the murder victim and a key prosecution witness. Pet. App. 94a–96a. Petitioners moved to quash the subpoenas on the basis that the SCA prohibited them from complying and that Defendants could obtain the content they sought by other means, including by subpoenaing the account holders directly. *Id.* at 96a.

The Superior Court denied Petitioners' motions to quash. Pet. App. 102a–06a. On review, the California Supreme Court ruled that communications accessible to the public implicitly fall under the SCA exception allowing for disclosure with the consent of the message's originator, and required Petitioners to produce any such public communications. *Id.* at 131a. With respect to communications accompanied by user-selected privacy restrictions, the court found that Section 2702(a) prohibited Petitioners from disclosing such communications, but did not reach the question whether constitutional interests could override the statutory prohibition. *Id.* at 134a–43a. The court then remanded for an evaluation of whether the SCA's consent exception applied to the particular communications sought in the subpoena, and whether "the proponents can obtain the same information by other means." *Id.* at 159a.

On remand, to narrow the scope of issues before the Superior Court, Petitioners produced public content to Defendants—i.e., Facebook, Instagram, and Twitter communications that the public could view. Pet. App. 59a; *see* 18 U.S.C. § 2702(b)(2). But Peti-

tioners objected to disclosing the remaining communications because the SCA, as interpreted by the California Supreme Court, explicitly prohibited them from doing so. Pet. App. 19a; *id.* at 6a. In addition to the statutory prohibition, the prosecution witness expressly instructed Petitioners *not* to disclose her private communications to Defendants. App. Vol. 6 at 1654–56, *Facebook, Inc. v. Superior Court*, No. A157902 (Cal. Ct. App. filed July 30, 2019). The Superior Court agreed with Petitioners that no SCA exception applied to those communications, but held that—notwithstanding the California Supreme Court's interpretation of the statute as prohibiting disclosure—the Defendants' Confrontation Clause and Due Process rights "both" "require[d] the production of" the "private posts" from the murder victim and prosecution witness. Pet. App. 65a. The Superior Court "order[ed] the service providers to produce these items." *Id.* at 63a.

Petitioners filed a petition for a writ of mandate and a stay of the production order on the grounds that the SCA barred the production of communications for which no statutory exception applied, and that Defendants' constitutional rights do not override the SCA's reasonable restriction on the gathering of evidence. *See* Petition 28–41, No. A157143 (Cal. Ct. App. filed May 8, 2019). The California Court of Appeal initially stayed the production order, Pet. App. 5a, but soon thereafter ordered that it would (1) entertain an appeal of the production order, but (2) dissolve the stay of the production order "notwithstanding any potential issues of mootness that could arise from the dissolving of [its] prior stay order," *id.* at 75a.

Petitioners immediately sought a further writ of mandate from the California Supreme Court. Petitioners explained that the Court of Appeal's order refusing to stay the production of the records at issue risked rendering appellate review of the production order moot. *See* Pet. App. 7a, 20a. The California Supreme Court initially reinstated a stay, but lifted that stay two weeks later while not addressing the lawfulness of that order. *Id.* at 72a.[1]

With no stay left in place, Petitioners had no choice but to be held in contempt to avoid violating the SCA and preserve appellate jurisdiction over the lawfulness of the production order. On July 26, 2019, the Superior Court ordered Petitioners in contempt of court for "[d]isobedience of [a] lawful judgment, order, or process of the court" and ordered Petitioners "to pay fines of $1,000 apiece, the maximum permitted by" state law. Pet. App. 7a–8a. Petitioners paid the fines and sought review of the contempt order in the Court of Appeal, along with return of the fine amounts. The Court of Appeal denied the writ. *Id.* at 2a. Facebook and Twitter then petitioned for review in the California Supreme Court on the same grounds. The California Supreme Court denied the petition. *Id.* at 1a.

REASONS FOR GRANTING THE PETITION

The lower courts are divided about whether a criminal defendant armed with a subpoena can force service providers to divulge electronic communications in violation of the Stored Communications Act. In California, following the decision below, service

---

[1] Petitioners' appeal of the production order remains pending in the Court of Appeal, even though the underlying criminal trial has already taken place. The Court of Appeal has not yet issued a decision.

providers who refuse to produce communications in response to criminal defendants' subpoenas face contempt if they fail to violate the SCA and turn over the communications. Other courts disagree, holding that Congress's unambiguous statutory prohibition on disclosure (absent an applicable exception not present here) must be followed and that the SCA poses no constitutional concerns for criminal defendants. *See Facebook, Inc. v. Wint*, 199 A.3d 625 (D.C. 2019); *State v. Bray*, 422 P.3d 250 (Or. 2018); *United States v. Pierce*, 785 F.3d 832 (2d Cir. 2015).

The split of authority has far-reaching ramifications. Millions of Americans send electronic communications over the Internet every day, and the SCA's unambiguous text and purpose shield those communications from access by unauthorized third parties, including criminal defendants. The California court's decision erodes the trust in the privacy of electronic communications instilled by the SCA. It prioritizes a criminal defendant's desire to obtain communications from whatever source she prefers—often without the knowledge of the people whose communications are at issue—despite the wishes of social media users who sent the messages and have not consented to sharing them. This result threatens to discourage the use and development of innovative technologies, in direct contravention of Congress's stated goal in enacting the SCA. Moreover, the decision below usurps Congress's role as the appropriate branch to make policy judgments on privacy issues, including how to accommodate criminal defendants' constitutional rights.

This Court should grant review.

I. THE LOWER COURTS ARE DIVIDED ON THE PRIVACY PROTECTIONS AFFORDED BY THE STORED COMMUNICATIONS ACT.

The Stored Communications Act's text is plain: Covered service providers "shall not knowingly divulge to any person or entity the contents" of electronic communications. 18 U.S.C. § 2702(a). Although Congress delineated certain statutory exceptions to this prohibition—including situations in which service providers "may" disclose communications (*id.* § 2702(b)) and other situations in which they are "require[d]" do so (*id.* § 2703)—there is no exception permitting disclosure to criminal defendants or other civil litigants armed with subpoenas.

Criminal defendants around the country, like Defendants in the proceedings below, have nevertheless attempted to avoid Congress's unambiguous prohibition by invoking their constitutional trial or due process rights. This has resulted in a divergence of opinions among the lower courts on whether Congress's prohibition can be overcome on such grounds. The California court's decision, allowing Facebook and Twitter to be held in contempt of court for refusing to violate the SCA and turn over electronic communications to a criminal defendant, departed from the decisions of two state courts of last resort and one federal court of appeals.

In *Facebook, Inc. v. Wint*, 199 A.3d 625 (D.C. 2019), the D.C. Court of Appeals unanimously reversed a contempt order that would have required Facebook to disclose a prosecution witness's electronic communications to a criminal defendant. Analyzing the SCA's statutory text and structure, the court explained that "[c]riminal defendants' subpoenas were not included by Congress in the list of exceptions, which

tends to support a conclusion that Congress did not intend to permit disclosure in response to criminal defendants' subpoenas." *Id.* at 632. And because "none of" the "nine enumerated exceptions" in Section 2702(b) applied, the court held that the "plain text of the SCA" "foreclose[s] Facebook from complying with [the criminal defendant's] subpoenas." *Id*. at 628. The court also rejected the defendant's invocation of "a constitutional right to obtain evidence for trial," supposedly rooted in the Due Process and Confrontation Clauses, holding that the defendant did not even "establish[ ] a serious constitutional *doubt*" as to the SCA's lawfulness. *Id.* at 633 (emphasis added).[2]

Likewise, the Oregon Supreme Court held that a criminal defendant could not assert constitutional rights to compel disclosures from service providers in contravention of the SCA. *State v. Bray*, 422 P.3d 250, 256 (Or. 2018). In *Bray*, the trial court granted a criminal defendant's motion to compel the State to use its

---

[2] The court's decision on the SCA's constitutionality is well-grounded in this Court's precedent. This Court has never recognized any constitutional right of criminal defendants to obtain pretrial discovery, and has repeatedly held that "[a] defendant's right to present relevant evidence is not unlimited, but rather is subject to reasonable restrictions." *United States v. Scheffer*, 523 U.S. 303, 306, 308 (1998) (holding that evidentiary rule that prohibited "the results of a polygraph examination" from being introduced at trial was not unconstitutional); *see also Pennsylvania v. Ritchie*, 480 U.S. 39, 52–53 (1987) (Confrontation Clause "does not include the power to require the pretrial disclosure of any and all information that might be useful" during a cross-examination); *Delaware v. Fensterer*, 474 U.S. 15, 20 (1985). In *Montana v. Egelhoff*, 518 U.S. 37 (1996), for example, this Court upheld a state law precluding the defense from offering evidence of voluntary intoxication, noting that "the proposition that the Due Process Clause guarantees the right to introduce all relevant evidence is simply indefensible." *Id.* at 42.

authority to obtain a victim's records from Google. *Id.* at 254. The State issued a subpoena that did not meet the SCA's requirements, so Google did not produce the information, and the State subsequently declined to seek a search warrant that complied with the SCA. *Id.* at 256. The Oregon Supreme Court held that a criminal "defendant, who is a nongovernmental entity, cannot require a remote computing service, such as Google, to divulge the contents of communications." *Id.* The court further held that "due process" rights "did not" "require[ ]" the State to assist the criminal defendant in obtaining information from service providers. *Id.* at 260. The Oregon Supreme Court noted that compelling Google to violate the SCA "was not the only means available to defendant to obtain evidence" he sought, and therefore the SCA's prohibition did not "constitute[ ] a due process violation." *Id.*

The Second Circuit also "reject[ed]" a criminal defendant's "claim" that the "SCA prohibited him from subpoenaing Facebook for page content, thereby denying him his Fifth Amendment due process right to present evidence and his Sixth Amendment right to confront adverse witnesses." *United States v. Pierce*, 785 F.3d 832, 841–42 (2d Cir. 2015). The Second Circuit explained that while Section 2703 of the SCA provides that "the government may obtain" the contents of communications through "a warrant, administrative subpoena, [or] court order," the "SCA does not, on its face, permit a defendant to obtain such information." *Id.* at 842. In holding that the criminal defendant suffered no "injury from the statute," the Second Circuit noted that the SCA's prohibition on service providers did not preclude criminal defendants from obtaining the information from other sources. *Id.* For example, the Sec-

ond Circuit observed, criminal defendants could subpoena the account holders themselves, who are "direct potential sources" for private information. *Id*.

In direct contrast, the California courts upheld a contempt order against providers who refused to violate the SCA on the basis that criminal defendants' constitutional rights "require[d]" the service providers to divulge private messages, notwithstanding Congress's express prohibition. Pet. App. 65a. The decision immediately garnered attention for its "unprecedented move" that "allowed the defense to obtain" posts on Facebook, Twitter, and Instagram. Maura Dolan, *After that $5-Billion Fine, Facebook Gets Dinged Again*, L.A. Times (July 26, 2019).

The press predicted that "criminal defense lawyers [we]re expected to cite the order in other cases where they are seeking access to private postings." Maura Dolan, *In Unprecedented Move, Facebook, Instagram, Twitter Ordered to Provide Private Posts in Gang Trial*, L.A. Times (July 18, 2019). That prediction proved accurate; criminal defendants have been quick to invoke the decision to justify subpoenas to service providers. *See* Def.'s Response to Facebook, Inc. Mot. to Vacate Preservation Order 5–6, *California v. Rocha*, No. 180118907 (S.F. Super. Ct. Aug. 27, 2019); Def.'s Opp. to Non-Party Facebook, Inc. Mot. to Quash 6–7, *California v. Harris*, No. 19012702 (S.F. Super. Ct. Nov. 1, 2019).

Further, the California court's decision has an outsized impact because California is the home of many social media companies, and therefore is a disproportionately likely forum for disputes over access to user communications. Unlike criminal defendants and private litigants in other states, California litigants can now seek to invoke constitutional trial and due process

rights to override Congress's determination that service providers "shall not" divulge communications. And service providers in California now must choose between turning over communications in violation of the SCA—therefore undermining the privacy interests of their users and risking significant civil liability—and subjecting themselves to a contempt order and sanctions.

This Court should grant review to resolve the conflict. Indeed, when this Court confronted a similar split of authority over the meaning of the SCA in *United States v. Microsoft Corp.*, 138 S. Ct. 1186 (2018) (per curiam), it granted review. In *Microsoft*, a district court held Microsoft in civil contempt for refusing to comply with a warrant issued under Section 2703 of the SCA seeking email contents stored abroad. *Id.* at 1187. A divided Second Circuit held that the disputed provision of the SCA does not apply extraterritorially and vacated the contempt finding. *Id.* This Court granted certiorari before dismissing the case as moot after Congress enacted an amendment to the SCA resolving the issue. *Id.* at 1187–88. The interests implicated by Defendants' interpretation of the SCA, in which they can gain access to private electronic communications through a mere subpoena, are no less important than the interests at stake in *Microsoft*, which involved a government's probable-cause-based warrant.

II. THIS CASE THREATENS THE PRIVACY INTERESTS OF MILLIONS OF AMERICANS.

The California court's decision undermines the scheme Congress enacted to protect the privacy of communications sent or received on electronic communications platforms—that is, the privacy interests of nearly all Americans.

Today, 90 percent of American adults use the Internet. Pew Research Ctr., *Internet/Broadband Fact Sheet* (June 12, 2019), https://tinyurl.com/wy3bh5h. The Internet "is vital for a wide range of routine activities in today's world," including "communicating with friends and family, and gathering information on just about anything." *United States v. LaCoste*, 821 F.3d 1187, 1191 (9th Cir. 2016); *see also Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018) (extending Fourth Amendment protection to data held by cell-phone providers because of the breadth of private information that can be obtained "[w]ith just the click of a button"); *Riley v. California*, 573 U.S. 373, 386 (2014) (extending warrant requirement to cell phones because of the "vast quantities of personal information" stored on phones and cloud storage).

Electronic communication services provided by companies like Petitioners—and others, such as Microsoft, Google, and Yahoo!—are "integral to the fabric of our modern society and culture." *Packingham v. North Carolina*, 137 S. Ct. 1730, 1738 (2017). Millions of Americans use service providers like Facebook and Twitter every day to communicate with friends, family, and other acquaintances. Such communications include not only social media "posts" that are widely accessible to a user's friends and followers, but also bilateral communications akin to text messages or email, using features like Facebook Messenger and Twitter direct messages. Facebook, *Messenger*, https://www.messenger.com/; Twitter, *About Direct Messages*, https://help.twitter.com/en/using-twitter/direct-messages; *see United States v. Freeze*, 784 F. App'x 203, 206 (5th Cir. 2019) (per curiam) (describing Facebook Messenger "conversation" between criminal defendant and victim). Because of the prevalence of

electronic communications, the SCA's Fourth Amendment-like protections—designed to ensure Americans can "lock away" their "personal and business information" just as effectively online as they can on paper, S. Rep. No. 99-541, at 3—are more important than ever.

As Internet use rises, "lawyers have increasingly looked to these social networks as litigation resources." Ryan A. Ward, *Discovering Facebook: Social Network Subpoenas and the Stored Communications Act*, 24 Harv. J.L. & Tech. 563, 564 (2011). And criminal "[d]efense lawyers" in particular "have been fighting to be able to have access to social media accounts to defend their clients." Maura Dolan, *California Supreme Court Says Social Media Firms Must Turn Over Some User Communications to Criminal Defendants*, L.A. Times (May 24, 2018); *see also*, *e.g.*, *United States v. Wenk*, 319 F. Supp. 3d 828, 829 (E.D. Va. 2017); *United States v. Nix*, 251 F. Supp. 3d 555, 559 (W.D.N.Y. 2017); *State v. Johnson*, 538 S.W.3d 32, 63 (Tenn. Crim. App. 2017).

After all, "the power to compel evidence from [Internet service providers] can be the power to compel the disclosure of a user's entire online world. Plus, disclosure can occur without notice to the user, and it can involve multiple accounts." Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 Colum. L. Rev. 279, 293 (2005). That is why the SCA directs criminal defendants to subpoena the person whose communications are sought, and not her service provider. When a subpoena is directed to the person who sent or received a message, video, or other communication, that person can make an informed choice whether to disclose or object to the subpoena based on her own privacy preferences. But when a

subpoena is directed to the person's service provider without notice to the person herself, she cannot take steps to protect her own privacy interests.

The California court's decision undermines the SCA in at least four distinct ways.

First, the decision undermines Congress's goal of protecting user privacy and ensuring that electronic communications are as safe as paper and telephone communications. Congress deliberately "placed providers in the position of protecting user data," and the SCA "exists because users expect providers to protect their information against involuntary production." Albert Gidari, *The Mandatory Emergency Disclosure Sinkhole Exception to the Email Privacy Act*, Ctr. for Internet & Society (May 24, 2016). Exposing users' communications to third parties who wish to use them in court contravenes the intent and expectations of people who use social media across the country.

In this case, for example, Petitioners were ordered to produce to criminal defendants on trial for murder a *crime victim's* and *prosecution witness's* electronic communications, despite the prosecution witness expressly instructing Petitioners *not* to disclose her communications to Defendants. App. Vol. 6 at 1654–56, *Facebook, Inc.*, No. A157902. This usurpation of user expectations, in turn, imposes a "disincentive to use an electronic service" to communicate—the very thing Congress sought to prevent in passing the law. H.R. Rep. No. 99-647, at 26; *see also* S. Rep. No. 99-541, at 5 (noting that a lack of legal protection for electronic communications "may unnecessarily discourage potential customers from using innovative communications systems"). It also has the potential to

subvert the criminal justice system; victims and government witnesses may be reluctant to come forward if it means criminal defendants will then be able to rifle through their social media accounts. *See* App. Vol. 3 at 1085–87, 1251, *Facebook, Inc.*, No. A157902 (information at issue potentially includes geolocation data of rival gang members).

Second, the decision exacerbates Congress's stated concern about "discourag[ing] American businesses from developing new innovative forms of telecommunications and computer technology." S. Rep. No. 99-541, at 5. If the California court's decision stands, service providers will be forced either to violate federal law or subject themselves to contempt of court. Forcing companies into this impossible position stifles innovation. *See Gun Owners' Action League, Inc. v. Swift*, 284 F.3d 198, 206 (1st Cir. 2002) (describing the "dilemma" of a "threatened prosecution" that puts the party "between a rock and a hard place" by forcing it to forgo lawful activity "or willfully violate the statute").

Third, allowing courts to say when a criminal defendant can override Congress's statutory choice raises separation of powers concerns. The legislative branch is best positioned to balance the multiple interests at stake, a principle this Court has recognized repeatedly in other contexts. *Salazar v. Buono*, 559 U.S. 700, 717 (2010) (plurality opinion) ("Congress's prerogative to balance opposing interests and its institutional competence to do so provide one of the principal reasons for deference to its policy determinations."); *Eldred v. Ashcroft*, 537 U.S. 186, 212–13 (2003) ("It is not our role to alter the delicate balance Congress has labored to achieve." (alterations omitted)); *Abrams v. Johnson*, 521 U.S. 74, 101 (1997)

("balancing the myriad factors and traditions" in districting "policies" "is best left to [the] legislatures"). Although Congress provided a safe harbor for service providers who rely in good faith on court orders, 18 U.S.C. § 2707(e)(1), that provision does not give courts license to order the production of information that would otherwise violate the SCA, as the court held in this case. Pet. App. 44a–45a. That circular logic would improperly give courts free rein to order violations of federal law whenever they believe a statutory exception *should* exist. *See Michigan v. Bay Mills Indian Cmty.*, 572 U.S. 782, 794 (2014) (courts "ha[ve] no roving license ... to disregard clear [statutory] language simply on the view that ... Congress 'must have intended' something broader"). Instead of adhering to Congress's judgment, the decision below contradicts it, opening the door to *ad hoc* judicial determinations about when to reject Congress's unambiguous dictate that service providers "shall not" divulge communications.[3]

Fourth, the decision represents a dramatic expansion of criminal defendants' constitutional "right to present a defense," Joshua A.T. Fairfield &

---

[3] Such judicially crafted exceptions to the SCA extend the import of the decision beyond the criminal context. By holding that a party's asserted litigation rights can "outweigh" the statute's prohibition on disclosure, Pet. App. 66a, the decision below cracks open the floodgates for civil litigants as well, who often seek to discover user communications that fall under the SCA. *See*, *e.g.*, *Mafille v. Kaiser-Francis Oil Co.*, No. 18-cv-586, 2019 WL 1933747, at *4 (N.D. Okla. May 1, 2019); *Katz v. Liberty Power Corp.*, No. 18-cv-10506, 2019 WL 957129, at *2–3 (D. Mass. Feb. 27, 2019); *Sines v. Kessler*, No. 18-mc-80080, 2018 WL 3730434, at *10 (N.D. Cal. Aug. 6, 2018); *PPG Indus., Inc. v. Jiangsu Tie Mao Glass Co.*, 273 F. Supp. 3d 558, 561 (W.D. Pa. 2017).

Erik Luna, *Digital Innocence*, 99 Cornell L. Rev. 981, 1064 (2014), jeopardizing the privacy protections not only of the SCA, but of other privacy-protective statutes like the Wiretap Act, 18 U.S.C. § 2516(1), that permit governmental access to private information while denying similar access to criminal defendants. *See* Rebecca Wexler, *Evidence in the Age of Privacy: Access to Data in the Criminal Justice System*, 67 UCLA L. Rev. (forthcoming 2020) (while asymmetrical exceptions to privacy laws are not uncommon, they do "raise conflicts between fairness for criminal defendants, trust in the adversary system, and the privacy interests of individuals who might not otherwise be involved in a criminal proceeding"); Stephanie Lacambra, *A Constitutional Conundrum That's Not Going Away—Unequal Access to Social Media Posts*, Electronic Frontier Foundation (May 31, 2018) (despite the "unfair[ness]" of the imbalance of power between prosecution and defense, courts "should not seek to correct it by sacrificing hard-won privacy protections"); Colin Fieman & Alan Zarky, *When Acquittal Is Just a Tweet Away: Obtaining Historical Social Media Evidence from Service Providers that Use the SCA as a Shield*, Champion 26 (Nov. 2015) (describing "the ever-increasing importance this type of information may hold for defendants"); Marc J. Zwillinger & Christian S. Genetski, *Criminal Discovery of Internet Communications Under the Stored Communications Act: It's Not a Level Playing Field*, 97 J. Crim. L. & Criminology 569, 571–72 (2007).

This Court's guidance is needed to resolve the important question whether the SCA's prohibition on disclosure must give way to a criminal defendant's asserted constitutional right to obtain evidence in support of his defense.

CONCLUSION

The petition for a writ of certiorari should be granted.

Respectfully submitted.

JAMES G. SNELL
PERKINS COIE LLP
3150 Porter Drive
Palo Alto, CA 94304
(650) 838-4300

JOHN R. TYLER
ANNA M. THOMPSON
PERKINS COIE LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101
(206) 359-8000

JOSHUA S. LIPSHUTZ
Counsel of Record
NAIMA L. FARRELL
AARON SMITH
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Avenue, N.W.
Washington, D.C. 20036
(202) 955-8500
jlipshutz@gibsondunn.com

MICHAEL J. HOLECEK
THOMAS F. COCHRANE
GIBSON, DUNN & CRUTCHER LLP
333 South Grand Avenue
Los Angeles, CA 90071
(213) 229-7000

Counsel for Petitioners

February 7, 2020